AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions and listings of claims in the application:

1. (Original) A method for intrusion detection, comprising:

receiving at a probe data packets communicated over a first network link;

converting the received data packets into a format suitable for a second network link;

monitoring, by the probe, the received packets to evaluate network performance; and

transmitting, by the probe over a second network link, data-converted packets to an intrusion detection system in communication with the second network link.

2. (Original) The method of claim 1 wherein the first network link is a WAN link and the second network link is a LAN.

3. (Original) The method of claim 1 wherein the method further comprises receiving, at a probe, data packets communicated over a third network link.

4. (Original) The method of claim 3, further comprising the step of aggregating the data packets received over the first network link and the data packets received over the third network link.

5. (Original) The method of claim 1 wherein the first network link operates using at least one HSSI protocol, T1 protocol, E1 protocol, ATM protocol, Packet-Over Sonet/SDH protocol, Frame-DS3 protocol, 1G Ethernet protocol, and 10G Ethernet protocol.

6. (Original) The method of claim 1 wherein the first network link comprises a protocol that encapsulates data traffic.

7. (Original) The method of claim 6 wherein the protocol comprises at least one of MPLS protocol, GMPLS protocol, VLAN (802.1q) protocol, HSSI protocol, T1 protocol, E1 protocol, ATM protocol, Packet-Over Sonet/SDH protocol, Frame-DS3 protocol, 1G Ethernet protocol, and 10G Ethernet protocol.

8. (Previously Presented) The method of claim 3, further comprising the step of maintaining, by the probe, an audit trail buffer for forensic analysis.

9. (Original) The method of claim 8 wherein the audit trail buffer comprises a memory for recording monitored packets.

10. (Original) The method of claim 9, wherein the memory records packets from at least one of the first network link and the third network link.

11. (Original) The method of claim 8, further comprising the steps of:

receiving, by the probe, an event notification; and

upon receipt of the event notification, communicating, by the probe, the current contents of the audit trail buffer.

12. (Original) The method of claim 1, wherein the converting step comprises:

storing received packets in a collection buffer;

stripping header information associated with a protocol of the first network link; and

adding header information associated with a protocol of the second network link.

13. (Original) The method of claim 12, wherein the step of storing comprises storing packets received from at least one of the first network link and a third network link.

14. (Currently amended) The method of claim 12 wherein:

the stripping step further comprises stripping ~~header and~~ checksum information associated with [[a]] the protocol of the first network link; and

the adding step further comprises adding ~~the header information and adding~~ checksum information associated with [[a]] the protocol of the second network link.

15. (Original) The method of claim 13, the step of stripping comprises stripping at least one of a Layer 2 MAC header, an Ethernet source address, and an Ethernet destination address.

16. (Canceled).

17. (Canceled).

18. (Canceled).

19. (Canceled).

20. (Canceled).

21. (Currently Amended) A network performance probe system comprising:

a first network interface for monitoring packets communicated over a first network link;

a packet converter for converting the monitored data packets into a format suitable for a second network link; and

a second network interface for communicating, over a second network link, converted packets to an intrusion detection system in communication with the second network link.

22. (Currently Amended) The network performance probe system of claim 21 further comprising a third network interface for monitoring packets communicated over a third network link.

23. (Currently Amended) The network performance probe system of claim 22 further comprising an aggregator for aggregating the packets from the first network link and the packets from the third network link.

24. (Currently Amended) The network performance probe system of claim 21 wherein the first network link comprises a WAN link and the second network link comprises an Ethernet.

25. (Currently Amended) The network performance probe system of claim 21 wherein the first network link operates using at least one HSSI protocol, T1 protocol, E1 protocol, ATM, Packet-Over Sonet/SDH protocol, Frame-DS3 protocol, and 10G Ethernet protocol.

26. (Currently Amended) The network performance probe system of claim 21 wherein the first network link comprises a protocol that encapsulates data traffic.

27. (Currently Amended) The network performance probe system of claim 26 wherein the protocol comprises at least one of MPLS protocol, GMPLS protocol, VLAN (802.1q) protocol, HSSI protocol, T1 protocol, E1 protocol, ATM protocol, Packet-Over Sonet/SDH protocol, Frame-DS3 protocol, 1G Ethernet protocol, and 10G Ethernet protocol.

28. (Currently Amended) The network performance probe system of claim 21, further comprising a performance analyzer for acquiring network performance data in response to the monitored packets communicated over the first network link.

29. (New) The network performance probe system of claim 22, wherein the probe further comprises an audit trail buffer maintainable for forensic analysis.

30. (Canceled).

31. (Canceled).

32. (Currently Amended) The network performance probe system of claim 29 wherein the audit trail buffer comprises a memory for recording monitored packets for forensic analysis.

33. (Currently Amended) The network performance probe system of claim 32, wherein the probe further comprises an event notification receiver for causing the probe, upon receipt of the event notification, to communicate the current contents of the audit trail buffer.

34. (Currently Amended) The network performance probe system of claim 21, wherein the converter comprises:

a collection buffer for storing received packets;

a stripper for stripping header information associated with a protocol of the first network link; and

an adder for adding header information associated with a protocol of the second network link.

35. (Canceled).

36. (Canceled).

37. (Canceled).

38. (Canceled).

39. (Canceled).

40. (Currently Amended) An article of manufacture comprising a program storage medium having computer readable program code ~~tangibly~~ embodied therein for providing intrusion detection, the computer readable program code in the article of manufacture including:

computer readable code for causing a computer to receive at a probe data packets communicated over a first network link;

computer readable code for causing a computer to convert the received data packets into a format suitable for a second network link;

computer readable code for causing a computer to monitor, via the probe, the received packets to evaluate network performance; and

computer readable code for causing a computer to transmit, via the probe over a second network link, data-converted packets to an intrusion detection system in communication with the second network link, so as to provide intrusion detection.

41. (Original) The article of manufacture of claim 40 wherein the program storage medium comprises a data signal embodied in at least one of ~~a carrier wave,~~ a computer magnetic disk, a computer optical disk, a tape, a non-volatile memory, a system memory, and a computer hard drive.

42. (Currently Amended) A program storage medium readable by a computer, ~~tangibly~~ embodying a program of instructions executable by the computer to perform method steps for providing intrusion detection, the method steps comprising:

receiving at a probe data packets communicated over a first network link;

converting the received data packets into a format suitable for a second network link;

monitoring, by the probe, the received packets to evaluate network performance; and

transmitting, by the probe over a second network link, data-converted packets to an intrusion detection system in communication with the second network link.

43. (Currently Amended) The program storage medium of claim 42 further comprising a data signal embodied in at least one of ~~a carrier wave,~~ a computer magnetic disk, a computer optical disk, a tape, a non-volatile memory, a system memory, and a computer hard drive.